From: James Madrid
Sent: Tuesday, June 30, 2020 10:41 AM
To: Timothy Stump
Subject: FW: Breach of Mostly Publishable Information

FYI

From: Rob Burford
Sent: Monday, June 29, 2020 8:46 AM
To: Francie Cordova <fcordova3@unm.edu>; Jeff Gassaway <base@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>
Subject: Breach of Mostly Publishable Information

Hello Francie and Jeff,

I just found out that there was a breach in an offsite server that houses information for UNMPD. I do not know the extent of what is on that server from UNMPD's stand point and copied James Madrid (as he will know if there is anything to be concerned about), but why I was apprised is that the Clery CSA information and hate bias stuff that goes through that server. Here are the things I see for these two items:

- The CSA's name, phone number, work address and email is what it captured via the CSA information, which is all public information anyway (unless they put down their personal cell phone number) – so does not seem like that is a problem.
- The CSA reports that get submitted through this platform could house information that is sensitive, which the only thing I see would be that of a victim of sexual assaults name being disclosed in a report or a student name being disclosed within in a report (which most of these reports do not have names attached because they are not asked for, except that of the reporting party). This is IPRA'able, as well, except the victim's name if disclosed, would be the biggest problem, as I mentioned.
- Hate Crime information submitted, all of this is IPRA'able, but student's names may have been disclosed here as names are asked for on this form, similar to above.

There are no social security number, birthdates, home addresses, credit card information, or other sensitive information that is collected for CSA information, but again do not know about the UNMPD side of things, which may be nothing.

Jeff or Francie, let me know if you have any questions and I can get you touch with my contact for UNMPD, who contracts with UNMPD.

Take care,

Rob Burford
Director of Compliance
141 Scholes Hall
(505)277-3979
rburford@unm.edu

From: James Madrid
Sent: Tuesday, June 30, 2020 10:41 AM
To: Timothy Stump
Subject: FW: Breach of Mostly Publishable Information

FYI

From: Jeff Gassaway
Sent: Monday, June 29, 2020 9:00 AM
To: Rob Burford <rburford@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>; Duane Ej Arruti <darruti@unm.edu>
Subject: Re: Breach of Mostly Publishable Information

Hi Rob,

Thank you for informing me; do you have the name or internet address of the server, or do you know who could get those for us?

Also, if this is something that the vendor will be performing the incident response (and any breach notification, if it's needed), that would be great, but please let us know if you need us to engage our information security and privacy office resource to assist in that.

I'm adding Duane to this to make him aware, in case we do need other resources.

- one quick question, what is a CSA?

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Monday, June 29, 2020 at 8:45 AM
To: Francie Cordova <fcordova3@unm.edu>, Jeff Gassaway <base@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>
Subject: Breach of Mostly Publishable Information

Hello Francie and Jeff,

I just found out that there was a breach in an offsite server that houses information for UNMPD. I do not know the extent of what is on that server from UNMPD's stand point and copied James Madrid (as he will know if there is anything to be concerned about), but why I was apprised is that the Clery CSA information and hate bias stuff that goes through that server. Here are the things I see for these two items:

- The CSA's name, phone number, work address and email is what it captured via the CSA information, which is all public information anyway (unless they put down their personal cell phone number) – so does not seem like that is a problem.
- The CSA reports that get submitted through this platform could house information that is sensitive, which the only thing I see would be that of a victim of sexual assaults name being disclosed in a report or a student name

being disclosed within in a report (which most of these reports do not have names attached because they are not asked for, except that of the reporting party). This is IPRA'able, as well, except the victim's name if disclosed, would be the biggest problem, as I mentioned.

- Hate Crime information submitted, all of this is IPRA'able, but student's names may have been disclosed here as names are asked for on this form, similar to above.

There are no social security number, birthdates, home addresses, credit card information, or other sensitive information that is collected for CSA information, but again do not know about the UNMPD side of things, which may be nothing.

Jeff or Francie, let me know if you have any questions and I can get you touch with my contact for UNMPD, who contracts with UNMPD.

Take care,

Rob Burford
Director of Compliance
141 Scholes Hall
(505)277-3979
rburford@unm.edu

From: James Madrid
Sent: Tuesday, June 30, 2020 10:42 AM
To: Timothy Stump
Subject: FW: Breach of Mostly Publishable Information

FYI

From: Rob Burford
Sent: Monday, June 29, 2020 9:02 AM
To: Jeff Gassaway <base@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>; Duane Ej Arruti <darruti@unm.edu>
Subject: RE: Breach of Mostly Publishable Information

Hello Jeff,

A CSA is a Campus Security Authority – we have to designate these as part of the Clery Act. I would reach out to James for that information for the information you asked for. I do not know your second question.

Take care,

Rob

From: Jeff Gassaway <base@unm.edu>
Sent: Monday, June 29, 2020 9:00 AM
To: Rob Burford <rburford@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>; Duane Ej Arruti <darruti@unm.edu>
Subject: Re: Breach of Mostly Publishable Information

Hi Rob,

Thank you for informing me; do you have the name or internet address of the server, or do you know who could get those for us?

Also, if this is something that the vendor will be performing the incident response (and any breach notification, if it's needed), that would be great, but please let us know if you need us to engage our information security and privacy office resource to assist in that.

I'm adding Duane to this to make him aware, in case we do need other resources.

- one quick question, what is a CSA?

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Monday, June 29, 2020 at 8:45 AM
To: Francie Cordova <fcordova3@unm.edu>, Jeff Gassaway <base@unm.edu>

Cc: James Madrid <jmadrid2@unm.edu>
Subject: Breach of Mostly Publishable Information

Hello Francie and Jeff,

I just found out that there was a breach in an offsite server that houses information for UNMPD. I do not know the extent of what is on that server from UNMPD's stand point and copied James Madrid (as he will know if there is anything to be concerned about), but why I was apprised is that the Clery CSA information and hate bias stuff that goes through that server. Here are the things I see for these two items:

- The CSA's name, phone number, work address and email is what it captured via the CSA information, which is all public information anyway (unless they put down their personal cell phone number) – so does not seem like that is a problem.
- The CSA reports that get submitted through this platform could house information that is sensitive, which the only thing I see would be that of a victim of sexual assaults name being disclosed in a report or a student name being disclosed within in a report (which most of these reports do not have names attached because they are not asked for, except that of the reporting party). This is IPRA'able, as well, except the victim's name if disclosed, would be the biggest problem, as I mentioned.
- Hate Crime information submitted, all of this is IPRA'able, but student's names may have been disclosed here as names are asked for on this form, similar to above.

There are no social security number, birthdates, home addresses, credit card information, or other sensitive information that is collected for CSA information, but again do not know about the UNMPD side of things, which may be nothing.

Jeff or Francie, let me know if you have any questions and I can get you touch with my contact for UNMPD, who contracts with UNMPD.

Take care,

Rob Burford
Director of Compliance
141 Scholes Hall
(505)277-3979
rburford@unm.edu

From: James Madrid
Sent: Tuesday, June 30, 2020 10:42 AM
To: Timothy Stump
Subject: FW: Breach of Mostly Publishable Information

FYI

From: Francie Cordova
Sent: Monday, June 29, 2020 9:02 AM
To: Rob Burford <rburford@unm.edu>; Jeff Gassaway <base@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>
Subject: RE: Breach of Mostly Publishable Information

Thanks for this Rob and to you Jeff for assistance in mitigation.

Francie

From: Rob Burford
Sent: Monday, June 29, 2020 8:46 AM
To: Francie Cordova <fcordova3@unm.edu>; Jeff Gassaway <base@unm.edu>
Cc: James Madrid <jmadrid2@unm.edu>
Subject: Breach of Mostly Publishable Information

Hello Francie and Jeff,

I just found out that there was a breach in an offsite server that houses information for UNMPD. I do not know the extent of what is on that server from UNMPD's stand point and copied James Madrid (as he will know if there is anything to be concerned about), but why I was apprised is that the Clery CSA information and hate bias stuff that goes through that server. Here are the things I see for these two items:

- The CSA's name, phone number, work address and email is what it captured via the CSA information, which is all public information anyway (unless they put down their personal cell phone number) – so does not seem like that is a problem.
- The CSA reports that get submitted through this platform could house information that is sensitive, which the only thing I see would be that of a victim of sexual assaults name being disclosed in a report or a student name being disclosed within in a report (which most of these reports do not have names attached because they are not asked for, except that of the reporting party). This is IPRA'able, as well, except the victim's name if disclosed, would be the biggest problem, as I mentioned.
- Hate Crime information submitted, all of this is IPRA'able, but student's names may have been disclosed here as names are asked for on this form, similar to above.

There are no social security number, birthdates, home addresses, credit card information, or other sensitive information that is collected for CSA information, but again do not know about the UNMPD side of things, which may be nothing.

Jeff or Francie, let me know if you have any questions and I can get you touch with my contact for UNMPD, who contracts with UNMPD.

Take care,

Rob Burford
Director of Compliance
141 Scholes Hall
(505)277-3979
rburford@unm.edu

From: James Madrid
Sent: Tuesday, June 30, 2020 10:44 AM
To: Timothy Stump
Subject: FW: Netsential Servers Compromised.

FYI

From: info@netsential.com [mailto:info@netsential.com]
Sent: Tuesday, June 30, 2020 7:33 AM
To: info@unmpd.org
Subject: Netsential Servers Compromised.

[EXTERNAL]

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: James Madrid
Sent: Tuesday, June 30, 2020 10:44 AM
To: Timothy Stump
Subject: FW: Netsential Servers Compromised.

FYI

From: Rob Burford
Sent: Tuesday, June 30, 2020 8:47 AM
To: Jeff Gassaway <base@unm.edu>; Duane Ej Arruti <darruti@unm.edu>
Cc: Francie Cordova <fcordova3@unm.edu>; James Madrid <jmadrid2@unm.edu>
Subject: FW: Netsential Servers Compromised.

Good Morning All,

Here is an email from Karen Fischer on the data breach that I mentioned yesterday. Netsential has a couple of questions for us below, to answer. I spoke with Karen Fischer this morning and we are going to do the following things to clean out the system and they are also going to do a dual factor authentication process to keep things even more secure. What we will do with the CSA piece:

- Is to deactivate all CSA's (Campus Security Authorities) that have not done what they have supposed to have done, as of June 1, 2019. This means some people will have to redo their information who are still CSA's, but have not updated as they should. Also, as a reminder, all the CSA information that may have been compromised is publishable, as it is work phone number, email and name. The only thing I can think of that might be an issue, is if they got passwords for logging into to be a CSA, then people would want to change their passwords to things, if they use the same for other log in items.
- I am asking for a list of CSA Reports from when they started housing the system, to see what kind of information has been identified (Again the only concerning thing would be student names, but we do not ask for names on these reports – only the name of the reporting party)
- I am also asking for a list of Hate Bias Reports – we do ask for names on this one and again the only issue would be the names of students that may have been disclosed within these reports.

The name of the Server is there and the contact for UNMPD is Karen Fischer, although the server is held by Stephen Gartrell sgartrell@netsential.com

Jeff, if you could let me know what else we may want to know, but please feel free to reach out to them, as I told Karen this morning that I have informed our IT Peeps (Jeff ☺) about this. A question for Jeff and/or Duane is that should we send a message to our CSA's about this or wait until we see what was disclosed? This way they can change their passwords, if you we think that is appropriate.

By the way, I think I am still ok with us using them, but that is up to others and to the PD. I am in the process of asking James Madrid on his thoughts on this, but have yet to actually talk to him.

Let me know what else you need to know from me.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 8:16 AM
To: Robert Burford <rburford@unm.edu>
Subject: Fwd: Netsential Servers Compromised.

[EXTERNAL]

fyi

---------- Original Message ----------
From: info@netsential.com
To: kfischer222@comcast.net
Date: 06/30/2020 7:33 AM
Subject: Netsential Servers Compromised.

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: James Madrid
Sent: Tuesday, June 30, 2020 10:56 AM
To: Timothy Stump
Subject: FW: Netsential Servers Compromised.

Importance: High

From: Jeff Gassaway
Sent: Tuesday, June 30, 2020 10:07 AM
To: Rob Burford <rburford@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>; James Madrid <jmadrid2@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: Lawrence Patrick Alderete <lpa@unm.edu>; Duane Ej Arruti <darruti@unm.edu>; Elaine Rising <erising@unm.edu>; Cinnamon Blair <cblair@unm.edu>
Subject: Re: Netsential Servers Compromised.
Importance: High

Hi Rob,

Thank you for getting additional details on this so we can develop our response approach. I have questions/ requests for individuals on this message.

- Commander Madrid, can you get us a copy of the original contract/ any renewals?
- Ari, we'd like to ask your assistance in evaluating any exposures we may have based on the Terms and Conditions in the contract/ amendments. We will likely need additional counsel and guidance on any breach response activities (though the vendor may be responsible for all of these).

I have copied Lawrence from our Security Operations team to review the initial information and (based on the contract and on Ari's guidance) develop a response for this incident.

I have copied Elaine Rising and Cinnamon Blair so that we can coordinate any communications using our incident and breach response templates we developed with OUC and UCAM.

My inclination is to immediately lock the CSA accounts and have a UNM employee with administrative access to the accounts validate the identities of CSA's before resetting passwords and initiating dual factor authentication, I think we should review what we know with security operations and determine whether we need to consider other actions before initiating those next steps. Hopefully we have UNM's next steps identified by late morning, but let's review and let the data we have inform that.

From a Personally Identifiable Information perspective, it seems like these are the two non-public data elements:

- names of incident reporting party and
- names of students disclosed in hate/ bias reports

One last note: it sounds like the vendor is uncertain as to whether they will stay in business as a result of this incident and their corresponding breach

Francie or Commander Madrid, in light of the uncertainty regarding this service provider, would either of you have the regulatory/ business requirements for this reporting software that we can share with internal IT folks to determine

- Does UNM have software licensed (or that is a possible add on) that meets these reporting requirements) or
- Does UNM have software developed that meets or that could meet these reporting requirements.

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Tuesday, June 30, 2020 at 8:46 AM
To: Jeff Gassaway <base@unm.edu>, Duane Arruti <darruti@unm.edu>
Cc: Francie Cordova <fcordova3@unm.edu>, James Madrid <jmadrid2@unm.edu>
Subject: FW: Netsential Servers Compromised.

Good Morning All,

Here is an email from Karen Fischer on the data breach that I mentioned yesterday. Netsential has a couple of questions for us below, to answer. I spoke with Karen Fischer this morning and we are going to do the following things to clean out the system and they are also going to do a dual factor authentication process to keep things even more secure. What we will do with the CSA piece:

- Is to deactivate all CSA's (Campus Security Authorities) that have not done what they have supposed to have done, as of June 1, 2019. This means some people will have to redo their information who are still CSA's, but have not updated as they should. Also, as a reminder, all the CSA information that may have been compromised is publishable, as it is work phone number, email and name. The only thing I can think of that might be an issue, is if they got passwords for logging into to be a CSA, then people would want to change their passwords to things, if they use the same for other log in items.
- I am asking for a list of CSA Reports from when they started housing the system, to see what kind of information has been identified (Again the only concerning thing would be student names, but we do not ask for names on these reports – only the name of the reporting party)
- I am also asking for a list of Hate Bias Reports – we do ask for names on this one and again the only issue would be the names of students that may have been disclosed within these reports.

The name of the Server is there and the contact for UNMPD is Karen Fischer, although the server is held by Stephen Gartrell sgartrell@netsential.com

Jeff, if you could let me know what else we may want to know, but please feel free to reach out to them, as I told Karen this morning that I have informed our IT Peeps (Jeff ☺) about this. A question for Jeff and/or Duane is that should we send a message to our CSA's about this or wait until we see what was disclosed? This way they can change their passwords, if you we think that is appropriate.

By the way, I think I am still ok with us using them, but that is up to others and to the PD. I am in the process of asking James Madrid on his thoughts on this, but have yet to actually talk to him.

Let me know what else you need to know from me.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 8:16 AM

To: Robert Burford <rburford@unm.edu>
Subject: Fwd: Netsential Servers Compromised.

[EXTERNAL]

fyi

---------- Original Message ----------
From: info@netsential.com
To: kfischer222@comcast.net
Date: 06/30/2020 7:33 AM
Subject: Netsential Servers Compromised.

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: James Madrid
Sent: Tuesday, June 30, 2020 10:56 AM
To: Timothy Stump
Subject: FW: Netsential Servers Compromised.

From: Lawrence Patrick Alderete
Sent: Tuesday, June 30, 2020 10:42 AM
To: Rob Burford <rburford@unm.edu>
Cc: Duane Ej Arruti <darruti@unm.edu>; Cinnamon Blair <cblair@unm.edu>; Francie Cordova <fcordova3@unm.edu>; Jeff Gassaway <base@unm.edu>; James Madrid <jmadrid2@unm.edu>; Elaine Rising <erising@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>
Subject: RE: Netsential Servers Compromised.

Mr. Burford,

Would it be possible for you to provide clarification regarding UNM's relationship with Karen Fischer?

Please advise.

-lpa

From: Jeff Gassaway <base@unm.edu>
Sent: Tuesday, June 30, 2020 10:07 AM
To: Rob Burford <rburford@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>; James Madrid <jmadrid2@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: Lawrence Patrick Alderete <lpa@unm.edu>; Duane Ej Arruti <darruti@unm.edu>; Elaine Rising <erising@unm.edu>; Cinnamon Blair <cblair@unm.edu>
Subject: Re: Netsential Servers Compromised.
Importance: High

Hi Rob,

Thank you for getting additional details on this so we can develop our response approach. I have questions/ requests for individuals on this message.

- Commander Madrid, can you get us a copy of the original contract/ any renewals?
- Ari, we'd like to ask your assistance in evaluating any exposures we may have based on the Terms and Conditions in the contract/ amendments. We will likely need additional counsel and guidance on any breach response activities (though the vendor may be responsible for all of these).

I have copied Lawrence from our Security Operations team to review the initial information and (based on the contract and on Ari's guidance) develop a response for this incident.

I have copied Elaine Rising and Cinnamon Blair so that we can coordinate any communications using our incident and breach response templates we developed with OUC and UCAM.

My inclination is to immediately lock the CSA accounts and have a UNM employee with administrative access to the accounts validate the identities of CSA's before resetting passwords and initiating dual factor authentication, I think we should review what we know with security operations and determine whether we need to consider other actions before initiating those next steps. Hopefully we have UNM's next steps identified by late morning, but let's review and let the data we have inform that.

From a Personally Identifiable Information perspective, it seems like these are the two non-public data elements:

- names of incident reporting party and
- names of students disclosed in hate/ bias reports

One last note: it sounds like the vendor is uncertain as to whether they will stay in business as a result of this incident and their corresponding breach

Francie or Commander Madrid, in light of the uncertainty regarding this service provider, would either of you have the regulatory/ business requirements for this reporting software that we can share with internal IT folks to determine

- Does UNM have software licensed (or that is a possible add on) that meets these reporting requirements) or
- Does UNM have software developed that meets or that could meet these reporting requirements.

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Tuesday, June 30, 2020 at 8:46 AM
To: Jeff Gassaway <base@unm.edu>, Duane Arruti <darruti@unm.edu>
Cc: Francie Cordova <fcordova3@unm.edu>, James Madrid <jmadrid2@unm.edu>
Subject: FW: Netsential Servers Compromised.

Good Morning All,

Here is an email from Karen Fischer on the data breach that I mentioned yesterday. Netsential has a couple of questions for us below, to answer. I spoke with Karen Fischer this morning and we are going to do the following things to clean out the system and they are also going to do a dual factor authentication process to keep things even more secure. What we will do with the CSA piece:

- Is to deactivate all CSA's (Campus Security Authorities) that have not done what they have supposed to have done, as of June 1, 2019. This means some people will have to redo their information who are still CSA's, but have not updated as they should. Also, as a reminder, all the CSA information that may have been compromised is publishable, as it is work phone number, email and name. The only thing I can think of that might be an issue, is if they got passwords for logging into to be a CSA, then people would want to change their passwords to things, if they use the same for other log in items.
- I am asking for a list of CSA Reports from when they started housing the system, to see what kind of information has been identified (Again the only concerning thing would be student names, but we do not ask for names on these reports – only the name of the reporting party)
- I am also asking for a list of Hate Bias Reports – we do ask for names on this one and again the only issue would be the names of students that may have been disclosed within these reports.

The name of the Server is there and the contact for UNMPD is Karen Fischer, although the server is held by Stephen Gartrell sgartrell@netsential.com

Jeff, if you could let me know what else we may want to know, but please feel free to reach out to them, as I told Karen this morning that I have informed our IT Peeps (Jeff ☺) about this. A question for Jeff and/or Duane is that should we send a message to our CSA's about this or wait until we see what was disclosed? This way they can change their passwords, if you we think that is appropriate.

By the way, I think I am still ok with us using them, but that is up to others and to the PD. I am in the process of asking James Madrid on his thoughts on this, but have yet to actually talk to him.

Let me know what else you need to know from me.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 8:16 AM
To: Robert Burford <rburford@unm.edu>
Subject: Fwd: Netsential Servers Compromised.

[EXTERNAL]

fyi

---------- Original Message ----------
From: info@netsential.com
To: kfischer222@comcast.net
Date: 06/30/2020 7:33 AM
Subject: Netsential Servers Compromised.

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: James Madrid
Sent: Tuesday, June 30, 2020 11:32 AM
To: Timothy Stump
Subject: FW: Netsential Servers Compromised.

FYI

From: Rob Burford
Sent: Tuesday, June 30, 2020 11:31 AM
To: Lawrence Patrick Alderete <lpa@unm.edu>
Cc: Duane Ej Arruti <darruti@unm.edu>; Cinnamon Blair <cblair@unm.edu>; Francie Cordova <fcordova3@unm.edu>; Jeff Gassaway <base@unm.edu>; James Madrid <jmadrid2@unm.edu>; Elaine Rising <erising@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>
Subject: Re: Netsential Servers Compromised.

Hello Lawrence,

Karen is contracted by UNMPD to assist with police items through their area. Clery (CSA's) became part of this when we started the Clery Coordinator position when Christine Chester held this role on an interim basis before I was hired into the role.

Hope this helps.

Take care,

Rob

From: Lawrence Patrick Alderete <lpa@unm.edu>
Date: Tuesday, June 30, 2020 at 10:41 AM
To: Robert Burford <rburford@unm.edu>
Cc: Duane Ej Arruti <darruti@unm.edu>, Cinnamon Blair <cblair@unm.edu>, Francie Cordova <fcordova3@unm.edu>, Jeff Gassaway <base@unm.edu>, James Madrid <jmadrid2@unm.edu>, Elaine Rising <erising@unm.edu>, Ariadna Vazquez <AriVazquez@salud.unm.edu>
Subject: RE: Netsential Servers Compromised.

Mr. Burford,

Would it be possible for you to provide clarification regarding UNM's relationship with Karen Fischer?

Please advise.

-lpa

From: Jeff Gassaway <base@unm.edu>
Sent: Tuesday, June 30, 2020 10:07 AM

To: Rob Burford <rburford@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>; James Madrid <jmadrid2@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: Lawrence Patrick Alderete <lpa@unm.edu>; Duane Ej Arruti <darruti@unm.edu>; Elaine Rising <erising@unm.edu>; Cinnamon Blair <cblair@unm.edu>
Subject: Re: Netsential Servers Compromised.
Importance: High

Hi Rob,

Thank you for getting additional details on this so we can develop our response approach. I have questions/ requests for individuals on this message.

- Commander Madrid, can you get us a copy of the original contract/ any renewals?
- Ari, we'd like to ask your assistance in evaluating any exposures we may have based on the Terms and Conditions in the contract/ amendments. We will likely need additional counsel and guidance on any breach response activities (though the vendor may be responsible for all of these).

I have copied Lawrence from our Security Operations team to review the initial information and (based on the contract and on Ari's guidance) develop a response for this incident.

I have copied Elaine Rising and Cinnamon Blair so that we can coordinate any communications using our incident and breach response templates we developed with OUC and UCAM.

My inclination is to immediately lock the CSA accounts and have a UNM employee with administrative access to the accounts validate the identities of CSA's before resetting passwords and initiating dual factor authentication, I think we should review what we know with security operations and determine whether we need to consider other actions before initiating those next steps. Hopefully we have UNM's next steps identified by late morning, but let's review and let the data we have inform that.

From a Personally Identifiable Information perspective, it seems like these are the two non-public data elements:

- names of incident reporting party and
- names of students disclosed in hate/ bias reports

One last note: it sounds like the vendor is uncertain as to whether they will stay in business as a result of this incident and their corresponding breach

Francie or Commander Madrid, in light of the uncertainty regarding this service provider, would either of you have the regulatory/ business requirements for this reporting software that we can share with internal IT folks to determine

- Does UNM have software licensed (or that is a possible add on) that meets these reporting requirements) or
- Does UNM have software developed that meets or that could meet these reporting requirements.

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Tuesday, June 30, 2020 at 8:46 AM
To: Jeff Gassaway <base@unm.edu>, Duane Arruti <darruti@unm.edu>
Cc: Francie Cordova <fcordova3@unm.edu>, James Madrid <jmadrid2@unm.edu>
Subject: FW: Netsential Servers Compromised.

Good Morning All,

Here is an email from Karen Fischer on the data breach that I mentioned yesterday. Netsential has a couple of questions for us below, to answer. I spoke with Karen Fischer this morning and we are going to do the following things to clean out the system and they are also going to do a dual factor authentication process to keep things even more secure. What we will do with the CSA piece:

- Is to deactivate all CSA's (Campus Security Authorities) that have not done what they have supposed to have done, as of June 1, 2019. This means some people will have to redo their information who are still CSA's, but have not updated as they should. Also, as a reminder, all the CSA information that may have been compromised is publishable, as it is work phone number, email and name. The only thing I can think of that might be an issue, is if they got passwords for logging into to be a CSA, then people would want to change their passwords to things, if they use the same for other log in items.
- I am asking for a list of CSA Reports from when they started housing the system, to see what kind of information has been identified (Again the only concerning thing would be student names, but we do not ask for names on these reports – only the name of the reporting party)
- I am also asking for a list of Hate Bias Reports – we do ask for names on this one and again the only issue would be the names of students that may have been disclosed within these reports.

The name of the Server is there and the contact for UNMPD is Karen Fischer, although the server is held by Stephen Gartrell sgartrell@netsential.com

Jeff, if you could let me know what else we may want to know, but please feel free to reach out to them, as I told Karen this morning that I have informed our IT Peeps (Jeff ☺) about this. A question for Jeff and/or Duane is that should we send a message to our CSA's about this or wait until we see what was disclosed? This way they can change their passwords, if you we think that is appropriate.

By the way, I think I am still ok with us using them, but that is up to others and to the PD. I am in the process of asking James Madrid on his thoughts on this, but have yet to actually talk to him.

Let me know what else you need to know from me.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 8:16 AM
To: Robert Burford <rburford@unm.edu>
Subject: Fwd: Netsential Servers Compromised.

[EXTERNAL]

fyi

---------- Original Message ----------
From: info@netsential.com
To: kfischer222@comcast.net
Date: 06/30/2020 7:33 AM
Subject: Netsential Servers Compromised.

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: Rob Burford
Sent: Tuesday, June 30, 2020 1:02 PM
To: KAREN FISCHER
Cc: Timothy Stump
Subject: Re: Files as per your request

Thanks for sending so quickly Karen.

Hope the rest of your day goes well.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 12:50 PM
To: Robert Burford <rburford@unm.edu>
Cc: Timothy Stump <tstump@unm.edu>
Subject: Files as per your request

[EXTERNAL]

Good Afternoon Rob,
As per your request, attached are spreadsheets with all CSA incidents submitted, CSA Smart incidents submitted, Public Hate/Bias incidents submitted and all CSA registrations. On the CSA registrations spreadsheet, there is a column that says CSA Status with either True or False beneath, the true are approved and the false indicates registrations that were never approved or have been deactivated. On the Public Hate/Bias incidents, the spreadsheet does not have any narrative that was included on the incident submitted, that information can be found on individual incidents, or if/when we provide all of the data submitted to UNM via files from Netsential at a later time.
Please let me know about any additional info that is needed.
Best,
Karen

From: KAREN FISCHER <kfischer222@comcast.net>
Sent: Tuesday, June 30, 2020 1:46 PM
To: Rob Burford
Cc: Timothy Stump
Subject: Re: Files as per your request

[EXTERNAL]

If/when you all want all of the data from their servers that have been databased since we started in around 2013, there could be additional details, but as far as these incidents go these should be complete, other than narratives that are not tied into the incident search that provided the data in the files I sent.

If you search on Nesential security breach in google, you can find out a lot more about what happened. I just did and it seems like there are many PD's, fusion centers, and other LE entities that have quite a bit of very sensitive info that has been compromised, and have a significant concern over the breach.
Let me know if you need anything else!
K

On 06/30/2020 1:02 PM Rob Burford <rburford@unm.edu> wrote:

Thanks for sending so quickly Karen.

Hope the rest of your day goes well.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 12:50 PM
To: Robert Burford <rburford@unm.edu>
Cc: Timothy Stump <tstump@unm.edu>
Subject: Files as per your request

[EXTERNAL]

Good Afternoon Rob,

As per your request, attached are spreadsheets with all CSA incidents submitted, CSA Smart incidents submitted, Public Hate/Bias incidents submitted and all CSA registrations. On the CSA registrations spreadsheet, there is a column that says CSA Status with either True or False beneath, the true are approved and the false indicates registrations that were never approved or have been deactivated. On the Public Hate/Bias incidents, the spreadsheet does not have any narrative that was included on the incident submitted, that information can be found on individual incidents, or if/when we provide all of the data submitted to UNM via files from Netsential at a later time.

Please let me know about any additional info that is needed.

Best,

Karen

From: Rob Burford
Sent: Tuesday, June 30, 2020 1:48 PM
To: KAREN FISCHER
Cc: Timothy Stump
Subject: Re: Files as per your request

Thanks for the update Karen.

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 1:45 PM
To: Robert Burford <rburford@unm.edu>
Cc: Timothy Stump <tstump@unm.edu>
Subject: Re: Files as per your request

[EXTERNAL]

If/when you all want all of the data from their servers that have been databased since we started in around 2013, there could be additional details, but as far as these incidents go these should be complete, other than narratives that are not tied into the incident search that provided the data in the files I sent.

If you search on Nesential security breach in google, you can find out a lot more about what happened. I just did and it seems like there are many PD's, fusion centers, and other LE entities that have quite a bit of very sensitive info that has been compromised, and have a significant concern over the breach.
Let me know if you need anything else!
K

> On 06/30/2020 1:02 PM Rob Burford <rburford@unm.edu> wrote:
>
> Thanks for sending so quickly Karen.
>
> Hope the rest of your day goes well.
>
> Take care,
>
> Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 12:50 PM
To: Robert Burford <rburford@unm.edu>
Cc: Timothy Stump <tstump@unm.edu>
Subject: Files as per your request

[EXTERNAL]

Good Afternoon Rob,

As per your request, attached are spreadsheets with all CSA incidents submitted, CSA Smart incidents submitted, Public Hate/Bias incidents submitted and all CSA registrations. On the CSA registrations spreadsheet, there is a column that says CSA Status with either True or False beneath, the true are approved and the false indicates registrations that were never approved or have been deactivated. On the Public Hate/Bias incidents, the spreadsheet does not have any narrative that was included on the incident submitted, that information can be found on individual incidents, or if/when we provide all of the data submitted to UNM via files from Netsential at a later time.

Please let me know about any additional info that is needed.

Best,

Karen

From: James Madrid
Sent: Tuesday, June 30, 2020 11:45 AM
To: Lawrence Patrick Alderete; Rob Burford
Cc: Duane Ej Arruti; Cinnamon Blair; Francie Cordova; Jeff Gassaway; Elaine Rising; Ariadna Vazquez; Timothy Stump
Subject: RE: Netsential Servers Compromised.

Hello Lawrence,

She is our main contact for Netsential, she is not an employee with UNM, just FYI for you.

Commander James A. Madrid
University of New Mexico Police Department
505-277-0231

"The only thing necessary for the triumph of evil is for good men to do nothing"
Edmund Burke

From: Lawrence Patrick Alderete
Sent: Tuesday, June 30, 2020 10:42 AM
To: Rob Burford <rburford@unm.edu>
Cc: Duane Ej Arruti <darruti@unm.edu>; Cinnamon Blair <cblair@unm.edu>; Francie Cordova <fcordova3@unm.edu>; Jeff Gassaway <base@unm.edu>; James Madrid <jmadrid2@unm.edu>; Elaine Rising <erising@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>
Subject: RE: Netsential Servers Compromised.

Mr. Burford,

Would it be possible for you to provide clarification regarding UNM's relationship with Karen Fischer?

Please advise.

-lpa

From: Jeff Gassaway <base@unm.edu>
Sent: Tuesday, June 30, 2020 10:07 AM
To: Rob Burford <rburford@unm.edu>; Ariadna Vazquez <AriVazquez@salud.unm.edu>; James Madrid <jmadrid2@unm.edu>; Francie Cordova <fcordova3@unm.edu>
Cc: Lawrence Patrick Alderete <lpa@unm.edu>; Duane Ej Arruti <darruti@unm.edu>; Elaine Rising <erising@unm.edu>; Cinnamon Blair <cblair@unm.edu>
Subject: Re: Netsential Servers Compromised.
Importance: High

Hi Rob,

Thank you for getting additional details on this so we can develop our response approach. I have questions/ requests for individuals on this message.

- Commander Madrid, can you get us a copy of the original contract/ any renewals?
- Ari, we'd like to ask your assistance in evaluating any exposures we may have based on the Terms and Conditions in the contract/ amendments. We will likely need additional counsel and guidance on any breach response activities (though the vendor may be responsible for all of these).

I have copied Lawrence from our Security Operations team to review the initial information and (based on the contract and on Ari's guidance) develop a response for this incident.

I have copied Elaine Rising and Cinnamon Blair so that we can coordinate any communications using our incident and breach response templates we developed with OUC and UCAM.

My inclination is to immediately lock the CSA accounts and have a UNM employee with administrative access to the accounts validate the identities of CSA's before resetting passwords and initiating dual factor authentication, I think we should review what we know with security operations and determine whether we need to consider other actions before initiating those next steps. Hopefully we have UNM's next steps identified by late morning, but let's review and let the data we have inform that.

From a Personally Identifiable Information perspective, it seems like these are the two non-public data elements:

- names of incident reporting party and
- names of students disclosed in hate/ bias reports

One last note: it sounds like the vendor is uncertain as to whether they will stay in business as a result of this incident and their corresponding breach

Francie or Commander Madrid, in light of the uncertainty regarding this service provider, would either of you have the regulatory/ business requirements for this reporting software that we can share with internal IT folks to determine

- Does UNM have software licensed (or that is a possible add on) that meets these reporting requirements) or
- Does UNM have software developed that meets or that could meet these reporting requirements.

Thank you,

Jeff

From: Robert Burford <rburford@unm.edu>
Date: Tuesday, June 30, 2020 at 8:46 AM
To: Jeff Gassaway <base@unm.edu>, Duane Arruti <darruti@unm.edu>
Cc: Francie Cordova <fcordova3@unm.edu>, James Madrid <jmadrid2@unm.edu>
Subject: FW: Netsential Servers Compromised.

Good Morning All,

Here is an email from Karen Fischer on the data breach that I mentioned yesterday. Netsential has a couple of questions for us below, to answer. I spoke with Karen Fischer this morning and we are going to do the following things to clean out the system and they are also going to do a dual factor authentication process to keep things even more secure. What we will do with the CSA piece:

- Is to deactivate all CSA's (Campus Security Authorities) that have not done what they have supposed to have done, as of June 1, 2019. This means some people will have to redo their information who are still CSA's, but have not updated as they should. Also, as a reminder, all the CSA information that may have been compromised is publishable, as it is work phone number, email and name. The only thing I can think of that might be an issue, is if they got passwords for logging into to be a CSA, then people would want to change their passwords to things, if they use the same for other log in items.
- I am asking for a list of CSA Reports from when they started housing the system, to see what kind of information has been identified (Again the only concerning thing would be student names, but we do not ask for names on these reports – only the name of the reporting party)
- I am also asking for a list of Hate Bias Reports – we do ask for names on this one and again the only issue would be the names of students that may have been disclosed within these reports.

The name of the Server is there and the contact for UNMPD is Karen Fischer, although the server is held by Stephen Gartrell sgartrell@netsential.com

Jeff, if you could let me know what else we may want to know, but please feel free to reach out to them, as I told Karen this morning that I have informed our IT Peeps (Jeff 😊) about this. A question for Jeff and/or Duane is that should we send a message to our CSA's about this or wait until we see what was disclosed? This way they can change their passwords, if you we think that is appropriate.

By the way, I think I am still ok with us using them, but that is up to others and to the PD. I am in the process of asking James Madrid on his thoughts on this, but have yet to actually talk to him.

Let me know what else you need to know from me.

Take care,

Rob

From: KAREN FISCHER <kfischer222@comcast.net>
Date: Tuesday, June 30, 2020 at 8:16 AM
To: Robert Burford <rburford@unm.edu>
Subject: Fwd: Netsential Servers Compromised.

[EXTERNAL]

fyi

---------- Original Message ----------
From: info@netsential.com
To: kfischer222@comcast.net
Date: 06/30/2020 7:33 AM
Subject: Netsential Servers Compromised.

Netsential web servers were recently compromised. We estimate the data breach was significant. At this time, the scope of information stolen is unknown. We are working with the appropriate law enforcement authorities regarding the intrusion and are fully cooperating with the ongoing investigation.

Although Netsential believes the software that runs your hosted website(s) is currently safe to use, we do not know the extent, sophistication or objectives of the hacker(s) and their ability to create future problems. It is recommended you immediately delete non-essential users and change all site access and email passwords.

The future of Netsential is uncertain. Please advise if you want us to continue to host and support your site(s) in order to minimize interruption to your operation.

Please contact us as soon as possible, but no later than July 10, 2020, at info@netsential.com, with your response/selection(s) to the below options.

1. Please continue to host and support our website(s) or specify date of cancelation.

2. Please transfer our website data to our organization. The contact information of the person to receive the electronic data must be provided.

Thank you for allowing us to serve you.

Any questions regarding this email, should be directed to info@netsential.com.

To remove yourself from this mailing list, Click here

From: KAREN FISCHER <kfischer222@comcast.net>
Sent: Tuesday, June 30, 2020 12:18 PM
To: Stephen Gartrell; Timothy Stump
Subject: Reset Passwords for unmpd.org

[EXTERNAL]

Hi Steve,
Can you proceed with a password reset for the UNM PD website as you mentioned was possible when we spoke earlier today? I am copying Commander Tim Stump, who is taking over from James Madrid, on this email so he can let his chain of command know that we have taken this action.
Thank you,
Karen

From: Rob Burford
Sent: Tuesday, June 30, 2020 1:47 PM
To: Timothy Stump; James Madrid
Subject: CSA Reports and Hate Bias Reports

Hey You Guys,

I can easily go through these, but may have some questions on the older ones, just to see if there is anything in the descriptions that would be concerning, but from the report information I do not seen anything that is a problem, initially on the CSA reports, but will look more into it tomorrow morning. I will also look at the Hate Bias stuff, there are far less than I thought there would be.

Take care,

Rob